GLBA and Cyber Risk Assessment

April 30, 2024

Assessment Methodology

The assessment involved a comprehensive review of the following information about the organization – assets that process sensitive data, technical and administrative controls, policies, and procedures. To ensure compliance with the Gramm-Leach-Bliley Act (GLBA), Tandem Cybersecurity, reviewed the Center for Internet Security (CIS) controls and the Federal Trade Commission's (FTC) GLBA safeguards.

The results of the control and safeguard review were used to conduct a risk assessment in accordance with GLBA requirements. This methodology allowed for a thorough evaluation of the organization's information security posture and helped to identify any gaps or vulnerabilities in its systems and practices. The assessment report provides recommendations for addressing identified risks and ensuring ongoing compliance with GLBA regulations.

GLBA
15 Key Elements/Safeguards

- Designation of a qualified individual for security program oversight.
- Conduct a written risk assessment.
- Implement and periodically review access controls.
- Know what you have and where you have it.
- Encrypt customer information, whether static or transit.
- Development of secure in-house or third-party apps to reduce risk to data.
- Implement two-factor authentication.
- Dispose of customer information securely.

GLBA
15 Key Elements/Safeguards Cont.

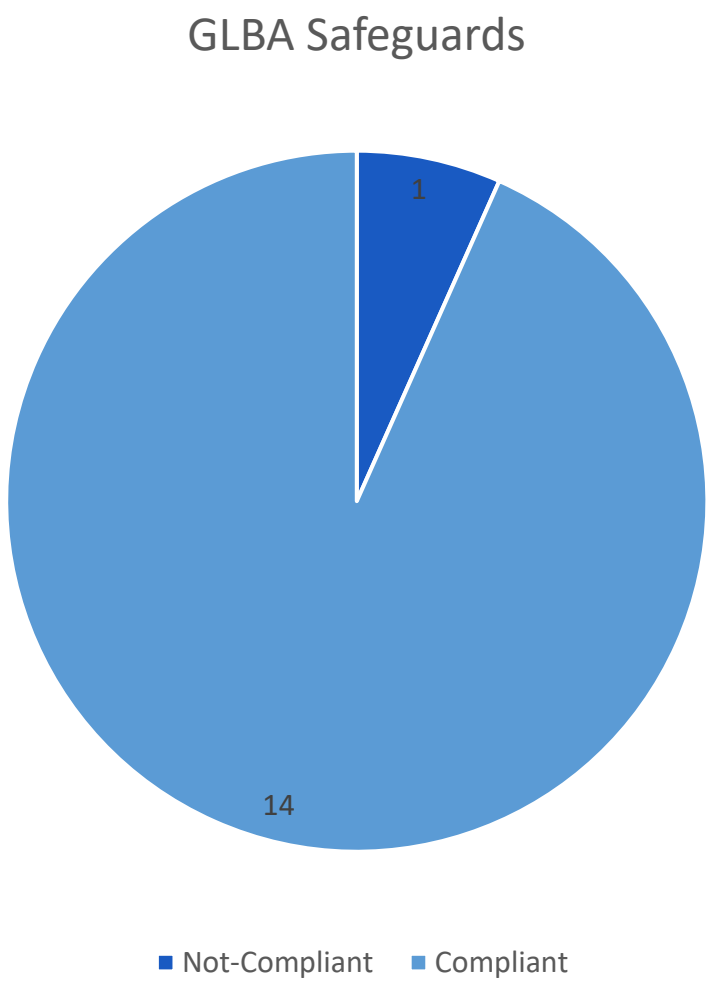
- Adoption of change management polices.
- Implementation of procedures and controls to monitor and log authorized user activity.
- Regularly monitor and test the effectiveness of your safeguards.
- Train employees regularly.
- Monitor service providers.
- Create a written Incident Response Plan.
- Mandatory reporting to Board of Directors (Trustees).

GLBA Assessment Overview

Out of the 15 Gramm-Leach-Bliley Act (GLBA) elements/safeguards, the college met 14. The reason 1 was only partially met, was establishing a consistent way to monitor our service providers and how they collect and meet protocol compliance in securing our data.

As a result, Barton's environment was uncompliant with the Gramm–Leach–Bliley Act Safeguards, and its risk level was determined to be **low** based on the applied CIS controls. Despite the non-compliance with the GLBA safeguards, the staff has implemented many safeguards to keep data secure. Other findings have a documented plan for action and associated milestones in the attached plan.

CIS controls (Implementation Groups 1 and 2) were also reviewed as part of the GLBA-required risk assessment.



Cyber Risk Assessment
CIS Controls

The CIS Critical Security Controls (CIS Controls) are a prioritized set of Safeguards to mitigate the most prevalent cyber-attacks against systems and networks. They are mapped to and referenced by multiple legal, regulatory, and policy frameworks.

There are 18 CIS Controls and within the 18 controls are 153 Safeguards. The 153 Safeguards are a set of specific, actionable measures designed to mitigate the most common and impactful cyber threats. Each Safeguard has a targeted "Asset Type" with a specific "Security Function".

The 18 CIS Critical Security Controls (cisecurity.org)

Control Safeguards list

We are working through Implementation Control Groups 1 and 2 and have fully or partially met 114 (97%) safeguards. The next risk assessment we will begin to step through Implementation Control group 3.

Cyber Risk Assessment
Findings and Recommendations

- DHCP Logging to Update Enterprise Asset Inventory
- Segment Data Processing Storage Based on Sensitivity
- Test Data Recovery
- Monitor Service Providers and Ensuring Third-party Vendors meet Security Expectations

Conclusion

Overall, the assessment discovered a few areas of concern and many compliant controls. The recommendations covered will ensure that Barton complies with critical cybersecurity controls meant to protect the scoped sensitive data.

Questions?